The Coastal Business Journal

Volume 17 | Number 1 Article 1

December 2019

The Strategic Problem of Information Security and Data Breaches

Michael Dinger
University of South Carolina Upstate

Julie Terrill Wade
University of South Carolina Upstate

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

The Strategic Problem of Information Security and Data Breaches

Michael Dinger, Johnson College of Business and Economics, University of South Carolina Upstate, 800 University Way, Spartanburg, SC 29303, mdinger@uscupstate.edu

Julie Terrill Wade, Johnson College of Business and Economics, University of South Carolina Upstate, 800 University Way, Spartanburg, SC 29303, mdinger@uscupstate.edu

ABSTRACT

This paper considers the strategic uncertainties and impacts created by high-profile data breaches and discusses the unique strategic problem presented by information security breaches for organizational executives. Based on theory regarding strategic uncertainties, we develop a framework depicting a strategic perspective on breaches within and outside the firm. Then, within the major categories outlined by the framework, this research evaluates instances of 17 public disclosures of high-profile data breaches over the past four years. Based on our discussion of these 17 cases, we identify six major issues complicating strategic decision-making regarding security breaches and discuss guidance for managers.

INTRODUCTION

Information security breaches are a serious problem for businesses across the world. Information security breaches can cause extensive damage, including the theft of corporate property, loss of corporate secrets and exposure of sensitive data (Bose & Leung, 2008; Crosman, 2014; Jensen, Dinger, Wright, & Thatcher, 2017; Weise, 2014a; Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Experts estimate that the average cost to a firm resulting from a security breach is $3.9 million (Ponemon, 2015, 2018), with security breaches at large organizations resulting in significantly higher costs. For example, a November 2013 security breach at Target cost the firm an estimated $148 million and a breach at Home Depot cost an estimated $62 million (Vinton, 2014). More recently, a massive breach at Equifax is believed to be the most costly in history, with direct costs exceeding $439 million and estimates that final costs may exceed $600 million (McCrank & Finkle, 2018).

In spite of the increasing prominence of information security breaches and their consequences, evidence suggests organizations are not adequately planning and preparing for cyber-attacks. A study by IBM finds that 77% of business leaders do not have an established cybersecurity incident response plan, and 57% of these leaders report that cyber incidents are taking longer to resolve (Forrest, 2018). Another study suggests that roughly half of key IT decision makers believe that their organization's top executives are not giving appropriate attention to IT security (Ismail,

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

2017). As a result, evidence suggests that many executives are not dedicating enough time and resources to properly support information security and to prepare for information security failures.

The purpose of this paper is to develop a framework to help managers and non-information technology (IT) executives understand the complexities and uncertainties surrounding data breaches in the modern business environment. To do so, we leverage theories of strategic uncertainty and environmental scanning (Allaire & Firsirotu, 1989; Courtney, Kirkland, & Viguerie, 1997; Elenkov, 1997). Models of scanning behavior suggest that executives scan their business environments for sources of strategic uncertainty, which are uncertainties within the environment perceived to potentially impact organizational performance (Elenkov, 1997). While many sources of strategic uncertainty are contingent on a firm's industry, such as the price of key raw materials for a manufacturer, we argue that information security breaches are unique because they represent a key source of strategic uncertainty for any business that uses information technology—which includes virtually all modern businesses. Combined with the lack of planning reported above, we believe it is necessary for executives to understand information security risks as a key source of strategic uncertainty and to plan accordingly.

To frame these strategic uncertainties for non-IT executives, we develop a high-level framework that depicts the strategic impacts of security breaches within the context of a dynamic business environment. Our intention is to highlight and frame issues that are relevant for non-IT executives to understand from a strategic point of view, but to avoid becoming overly entangled in technical complexities.

To develop the framework, we sought to gather data from firms that experienced security failures. Due to the sensitive nature of security breaches and potential legal ramifications for breached firms, collecting primary data via interviews or surveys directly from recently breached firms is impractical. As a result, we leverage secondary data. We identified 17 major security breaches from 2014-2017 (see Table 1) and reviewed these cases to develop the framework and implications discussed in this paper.

Our contribution is threefold. First, for non-IT executives, we provide high-level guidance regarding the unique strategic uncertainties related to IT security, intending to drive thoughtful conversation with IT staff when making appropriate security-related decisions. Second, for IT personnel, we provide a framework that may be useful when explaining and justifying security-related investments to organizational executives. Third, for academics, we intend for the framework and issues discussed in this paper to highlight interesting and novel paths of research in the areas of strategic management and information systems.

The paper proceeds as follows: First, we develop a conceptual framework to provide a high-level perspective on IT operational failures, strategic impacts and environmental influences. Next, we leverage the conceptual framework to discuss six specific issues of interest to business executives, along with practical guidance to help executives discuss appropriate responses with IT

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

personnel. Finally, we conclude with a discussion of limitations and suggestions for future research.

Table 1: Summary of Major Security Breaches 2014-2017 Reviewed

Organization	Year Disclosed	Size of Breach	Source(s)
Anthem	2015	80 million customers	(Collins, 2015; Vinton, 2015)
Ashley Madison	2015	32 million user accounts	(Thomsen, 2015; Zetter, 2015b)
Community Health Systems	2014	4.5 million patients	(McCarthy, 2015; Weise, 2014b)
eBay	2014	145 million user accounts	(Collins, 2015; McCarthy, 2015; Reisinger, 2014)
Equifax	2017	147 million Americans	(Fung, 2018; O'Brien, 2017)
Home Depot	2014	56 million customers	(Collins, 2015; McCarthy, 2015; Vinton, 2014)
JPMorgan Chase	2014	76 million customers 7 million small businesses	(Collins, 2015; McCarthy, 2015; Reuters, 2014)
LinkedIn	2016	167 million user accounts	(Hackett, 2016)
Premera Blue Cross	2015	11 million customers	(Collins, 2015; Vinton, 2015)
Sony Pictures	2014	47,000 employees	(Collins, 2015; Pagliery, 2014; Roettgers, 2015)
Target	2014	40 million customers	(Collins, 2015; Vinton, 2014)
Tumblr	2016	65 million user accounts	(Kovacs, 2016)
Uber	2017	57 million driver and rider accounts	(Issac, Benner, & Frenkel, 2017; Newcomer, 2017)
Verizon	2016	1 million enterprise customers	(Narcisi & Kuranda, 2016)
Yahoo	2016	500 million user accounts	(Fiegerman, 2016a)
Yahoo	2016	1 billion user accounts	(Fiegerman, 2016b)
Yahoo	2017	3 billion user accounts	(Larson, 2017)

CONCEPTUAL FRAMEWORK

Organizations operate under conditions of uncertainty (Allaire & Firsirotu, 1989; Courtney et al., 1997; Elenkov, 1997). Executives engage in scanning behavior to identify strategic uncertainties that significantly affect the future performance of the organization (Elenkov, 1997). Strategic uncertainties vary significantly from industry to industry and business to business, as factors that may dramatically impact one business may not impact another (e.g., industry-related

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

legislation, availability of distribution channels, price of key raw materials or consumer trends). Given the ubiquity of information technology and the extent to which it is embedded across almost all industries, we suggest that information security-related risks are unique in that they represent key sources of strategic uncertainty for virtually all modern businesses that leverage information technology.

Research posits four increasing levels of strategic uncertainty (Courtney et al., 1997). Level 1, or low uncertainty, suggests a rather clear future where events are relatively predictable. Level 2 implies a set of discrete alternatives (i.e. three distinct possible outcomes), where the future may consist of distinct and identifiable paths. Level 3 indicates a range of futures determined by different variables, and that future outcomes lie along a continuum rather than discrete outcomes, and the outcomes vary according to the strength and influence of each variable. Level 4 represents true ambiguity where the future cannot reasonably be predicted due to extremely high levels of uncertainty (Courtney et al., 1997). Accordingly, as the level of strategic uncertainty increases, the ability to engage in strategic planning and analysis becomes more difficult.

We suggest that strategic uncertainties surrounding information security exist at Level 3. The possible outcomes of information security failures are generally well known and established, but do not exist in easily categorized discrete outcomes. The consequences of information security failures vary according to many different factors, such as the extent and nature of data lost, how quickly the breach was identified and addressed, whether the breach impacted business partners, the malicious intentions of the attacker, and so forth. Accordingly, understanding the nature of information security risks and planning accordingly is a difficult task, especially for organizational executives who often lack a highly technical background. This is an especially critical task, though, since roughly half of IT personnel report that executives do not give IT security enough attention (Ismail, 2017) and IBM reports that about 3/4ths of organizations do not have necessary IT security plans in place (Forrest, 2018).

Chief executives are in a precarious position regarding information security strategy and managing these strategic uncertainties. Top management personnel are in the best position to make decisions regarding information security strategy and the level of investment in security (Ross & Weill, 2002; Weill & Ross, 2004), yet strategic decisions regarding information security are often a decision-making quandary for top executives. On one hand, decisions to enhance and pursue higher levels of information security may effectively minimize risks associated with security breaches and data leaks. This direction may be in the best ethical interest of various stakeholders in the firm, including employees and customers. On the other hand, the decision to extensively pursue and heavily invest in higher levels of information security may actually run cross purposes with organizational and strategic goals. Over emphasizing security may draw a firm's attention away from strategic initiatives that offer greater potential for growth and profitability (Ocasio, 1997; Ocasio & Joseph, 2005) or may limit a firm's ability to create customized and proprietary information technology products and services (Anderson, 2001).

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

Security-related decision-making and the consequences of data breaches do not occur in isolation. To frame the relationship, we depict a conceptual framework in Figure 1. Although far more specific and granular taxonomies of information security threats have been developed (e.g., Cebula & Young, 2010), we opt to develop a higher level conceptual framework to depict issues at a more strategic level, as opposed to a discussion of threats that might be more technical than many managers and executives may find practical.

At the center of the figure, we see two firms. Within each firm, we consider the risks and consequences directly associated with each firm's own IT operational failures and the direct strategic impacts of operational failures. Although our interest focuses specifically on data breaches, we use the term IT operational failure in the figure to more broadly include a variety of situations where IT-related failures may have significant consequences and to provide a framework useful for other avenues of research. Numerous taxonomies exist depicting the variety of IT operational failures; these potential cyber security risks include the actions of people, system and technology failures, internal process failures and external events, such as fires or natural disasters (Cebula & Young, 2010).

We consider that each firm's own operational failures may cause immediate and direct strategic consequences for the firm, as depicted by the arrow flowing upwards. For example, during Amazon's "Prime Day" shopping event, the Amazon website experienced technical glitches over the first hours and estimates suggest the malfunctions cost Amazon nearly $100 million in sales (Korosec, 2018). Of course, as discussed heavily above, large scale data breaches often have major repercussions for firms in terms of revenue and brand image.

Additionally, we consider that IT operational failures (i.e., security breaches) at other firms may directly result in enhanced attacks on another firm's IT operations, as depicted by the two-way arrow between the two firms at the IT operational level. For example, hackers were able to gain entrance to Target's information systems after garnering user credentials from Fazio Mechanical Services, a refrigeration, heating and air conditioning subcontractor (Krebs, 2014). Furthermore, consider the problem of password re-use by users, and how password credentials stolen through another security breach might be used to target user accounts within another firm if the users re-use the same password (Ives, Walsh, & Schneider, 2004). Additionally, consider that security breaches within a firm might result in cyber-attackers using the breach to enable an attack on a business partner—exposing the initial firm to even more liability, or at least a damaged relationship with a business partner. As a result, we reinforce the notion that firms, and their IT operations, do not exist in isolation, but firms are influenced indirectly and directly by the operational failures and consequences of other firms.

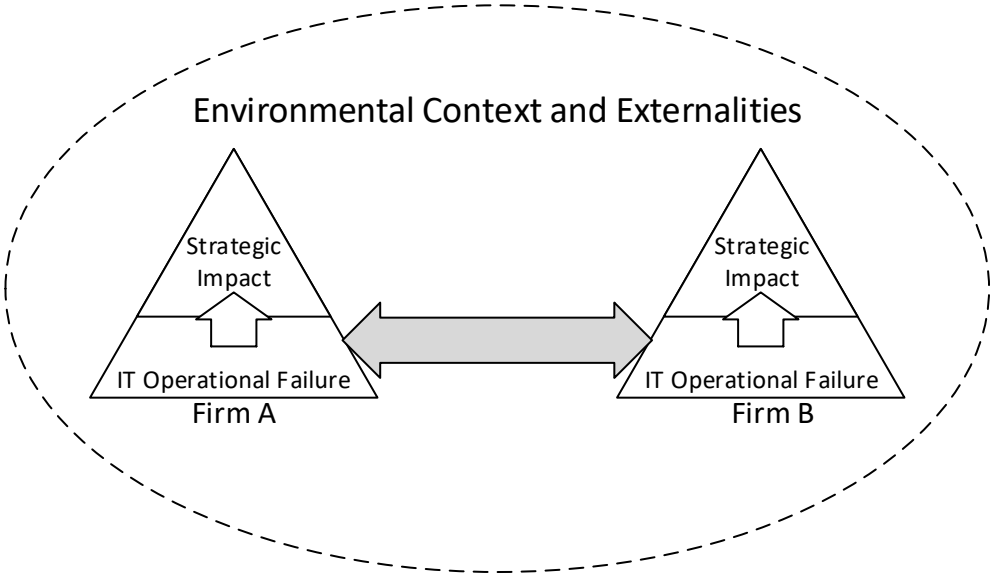
Finally, we consider that firms do not exist in isolation but operate and compete in a modern marketplace where they influence, and are influenced by, customers, competitors, business partners, regulatory agencies and other external actors and forces. Broadly speaking, major actions or events experienced by the firm may influence others in the environment while the environment simultaneously impacts the firm (Jones & Karsten, 2008) as depicted by positioning each firm

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

within the environmental context and externalities. For example, the 2017 Equifax breach, wherein sensitive personal information, including social security numbers, names and addresses, on 147 million Americans was exposed (O'Brien, 2017) occurred in a context where hundreds of millions of individuals had already experienced losing user account data (e.g., eBay, Yahoo and LinkedIn breaches), healthcare-related personal information (e.g., Anthem, Community Health Systems and Premera Blue Cross breaches), and credit card information (e.g., Target and Home Depot breaches). Had the Equifax breach occurred a decade ago before data breaches were commonplace, the revelation might have been shocking to stakeholders, including customers, business partners and investors, with devastating consequences for Equifax's ability to continue operations. Instead, in spite of the most expensive data breach ever (McCrank & Finkle, 2018), such breaches appear to be "business as usual" with firms not experiencing crippling long-term consequences—as we discuss in more depth later in this paper.

Figure 1. Conceptual Framework



In summary, the key takeaways of the proposed framework are as follows: First, IT operational failures, such as data breaches, have various consequences. Those consequences might include a wide range of outcomes, including additional cyber-attacks within the firm or on other firms as well as direct and indirect strategic impacts. Second, we suggest that IT operational failures permeate into the general environment in which the firm operates and that the continually changing external environment contextualizes the consequences of operational failures within a firm based on other breaches and failures that have occurred and continue to occur in the environment.

CASE ANALYSIS

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

There are numerous factors at work in the discussion of information security investments. Almost none of these factors are straightforward or simple to interpret which vastly complicates the decision-making process. Based on analysis of the 17 breaches previously identified, the following sections frame six major issues based on our conceptual framework (see Figure 1) demonstrating why information security issues are such challenging and complex strategic uncertainties for executives. We identify two major issues based on IT Operational Failures, two based on Strategic Impacts and two based on Environmental Context and Externalities. After discussing each issue, we provide general guidance for managers and decision-makers.

IT Operational Failures

1. Information security must protect everywhere, but cyber-attackers only need one weakness.

IT operational failures represent a key source of strategic uncertainty for organizations, and security failures are a significant source of risk (Goldstein, Chernobai, & Benaroch, 2011). In dealing with this source of risk, a primary problem among security personnel is the game of "cat and mouse" between an organization's security personnel and the cyber-attackers intent on compromising the organization's systems. Security personnel must find and patch every security flaw while the attackers need only find one significant flaw, which puts security personnel in the position of needing to be comprehensive and verify that there are no vulnerabilities. As security researcher Ross Anderson writes:

> So information warfare looks rather like air warfare looked in the 1920s and 1930s. Attack is simply easier than defense. Defending a modern information system could also be likened to defending a large, thinly-populated territory like the nineteenth century Wild West: the men in black hats can strike anywhere, while the men in white hats have to defend everywhere. (p. 5, Anderson, 2001)

Ultimately, security breaches result from a wide variety of sources, including from breaches at business partners, customers or suppliers. In the attack on Target, the intruders first breached one of Target's vendors, Fazio Mechanical Services, an HVAC service provider, and then used Fazio's vendor credentials to access Target's systems (Krebs, 2014). In yet another type of threat, an executive at Ashley Madison speculated that their data breach resulted from an inside job and was perpetrated, at least in part, by an individual with access to organizational systems (Krebs, 2015). Other breaches result from more direct attacks on organizational systems, such as the Home Depot data breach, which was enabled by malware designed to steal credit and debit card information from point of sale systems (Vinton, 2014). Other attacks on Anthem, Community Health Systems and Premera Blue Cross also purportedly used malware designed to gain access to systems and expose personal medical data to the attackers. The many possible attack vectors create a significant source of uncertainty for security personnel.

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

The need for comprehensive security is a significant problem because it places organizations in the position of having to constantly identify key weaknesses from a wide range of possibilities and to shore up those weaknesses before cyber-attackers can identify and capitalize on them. As a result, decision makers have to consider both technical and human security weaknesses.

In order to counteract the continuing threat of security breaches, management needs to engage in active risk management processes. Risk management is an approach to handling strategic uncertainties (K. D. Miller, 1992) and addresses the process of identifying and analyzing risks, then implementing appropriate risk management plans to minimize the potential damages of the identified risks (Boehm, 1991). After identifying relevant risks, four risk management options include (1) risk avoidance, (2) risk transference, (3) risk reduction, and (4) risk acceptance (Blakley, McDermott, & Geer, 2001; Boehm, 1991). We discuss each of these options in more detail below.

First, managers can choose to alter plans and processes to avoid risks, such as not collecting consumer data or allowing consumers to create user accounts in order to avoid losing their data and any associate liability. Second, managers can choose to transfer risks to another party, either through outsourcing operations or by purchasing insurance. For example, managers might outsource customer relationship management processes to a vendor in order to avoid risks associated with security liabilities. Alternatively, managers might hire an outside firm to manage IT security processes with the expectation that fallout from security breaches fall to the IT security provider. To transfer financial risk, a firm may buy insurance against security breach damages. For instance, Equifax received $125 million from insurance to help defray the cost of their recent breach (McCrank & Finkle, 2018). Third, firms might invest heavily in information security, such as improved technology, investments in personnel, or enhanced policies, in order to reduce the risk of security breaches. Fourth, firms may simply acknowledge that the risk exists and accept the associated risk of damage, but choose not to avoid, transfer or reduce the risk. In this case, firms might set aside funding to pay for associated damages in the event that breaches do occur.

Although a comprehensive guide to risk management is beyond the scope of this paper, useful guides are available to help manage and frame organizational response to key uncertainties (see for example Boehm, 1991). Depending on the size of the organization and resources available, executives may choose to hire vendors to engage in risk management planning, hire or assign personnel to address risk management, or engage in risk management planning personally. The level of resource investment in risk management planning should be commensurate with the perceived level of risk the organization attaches to their IT operations.

2. Information security requires extensive technical security, yet human security failures can bypass even sophisticated technical security.

Organizations that choose to invest in mitigating the significant threat posed by security breaches rely on technological interventions, such as a comprehensive suite of information technology and security tools, including use of passwords, firewalls, antivirus, encryption and

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

blocking/filtering technologies and more. These tools are necessary to protect against common threats, such as direct network intrusions, the illicit monitoring of unsecured communications, and attacks via malware, worms or viruses. However, strong security technology is a necessary, but not sufficient, condition to prevent security breaches.

The human element of information security magnifies the uncertainties attached to information security. The situation is reminiscent of the classic urban legend scenario where a baby sitter is repeatedly harassed by a threatening caller, and when they police trace the phone call, they realize the calls are coming from *inside* the house. For organizations, security risks and failures often come from *inside* the organization due to human failures.

Whereas the technology tools used for security may be circumvented or overcome, their technological nature means the tools operate in a relatively consistent and predictable way. The human users of organizational information systems play a critical role in maintaining information security, but are much less consistent and predictable (Wright et al., 2014). In spite of the strength of information security measures, if system users surrender login credentials or inadvertently install malicious software on their computers, technical security features can be bypassed and rendered ineffective. For instance, in a cyber-attack on defense contractor Booz Allen Hamilton, an executive was sent an email with an attachment ostensibly containing details from the Pentagon (Grow, Epstein, & Tschang, 2008). Though appearing credible, the email attachment contained malware that, if opened, was designed to track the user's keystrokes and to provide access to the cyber-attacker.

In fact, social engineering is a noted intrusion technique (Mitnick & Wimon, 2005). Social engineering targets system users or organizational employees as a key weakness in a security system and capitalize on psychology and influence techniques to elicit compliance from system users in an attempt to fool them into revealing login credentials, install malicious software, or otherwise provide further access and control to the cyber-attacker. As a result, users and IT personnel must be ever vigilant against the threat of cyber-attack. Organizations therefore need interventions to prepare and encourage users to remain vigilant against such threats.

In order to counteract the threat of human vulnerabilities, organizations need to regularly engage in current information security training and to create and encourage users to comply with information security policies (Bulgurcu, Cavusoglu, & Benbasat, 2010; Puhakainen & Siponen, 2010; Siponen, Mahmood, & Pahnila, 2014). Information security policies should be developed and communicated to employees to establish safeguards against access by unauthorized users and loss of data assets. While generic information security policy templates are widely available, firms should engage in development of custom firm-specific policies to the extent that their operations or data assets are idiosyncratic or highly valuable. Furthermore, at the very least, users should be trained on how to recognize common social engineering attacks, such as phishing and spear phishing, which are commonly used to try to steal credentials and access proprietary information (Jensen et al., 2017). While traditional anti-phishing training focused on memorizing sets of rules, more current approaches support embedded training with simulated phishing emails (Kumaraguru

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

et al., 2009) or training users to think more mindfully about suspicious emails and what they ask of the recipient (Jensen et al., 2017).

For executives to effectively engage in risk management regarding the strategic uncertainties attached to information security, they must understand that even the most sophisticated technological interventions can be undermined by oblivious or under-trained users within the organization. In other words, even the most sophisticated security measures can be undone by users mindlessly but willingly giving away sensitive data to a well-designed attack. As a result, executives should understand that a comprehensive plan to manage risks involves appropriate investment in the organization's human capital through training and development in conjunction with investment in technological capital. This is particularly crucial for executives to understand, since research indicates that top management support for training contributes to training effectiveness (Cromwell & Kolb, 2004; Facteau, Dobbins, Russell, Ladd, & Kudisch, 1995).

Strategic Impacts

3. Security breaches have immediate financial consequences, but long-term financial damages may be limited depending on the nature of the breach.

After experiencing security breaches, firms face immediate costs such as identifying the source of the breach, resolving the security weakness, paying regulatory fines, absorbing the cost of class action lawsuits and paying reparations for damages to customers, employees or partners. There may also be long-term and harder to quantify damages in terms of harm to a reputation or lost revenue that may significantly damage a firm's ability to compete in the marketplace. The inability to quantify the various costs magnifies the level of strategic uncertainty attached to IT security risks. At face value, the financial damages of security breaches are significant. In fact, one report suggests that 60% of small businesses go bankrupt within 6 months of a cyber-attack (Miller, G., 2016), which is understandable in light of recent analyses suggesting that the cost of the average security breach has risen over the past several years to an average of $3.9 million (Ponemon, 2015, 2018). Table 2 reports the available estimated direct costs for the security breaches we identified for this study.

Table 2: Estimated Direct Cost of Security Breaches

Organization	Estimated Direct Cost	Source
Anthem	>$100 million	(Osborne, 2015)
Community Health Systems	>$100 million	(McGee, 2014)
Equifax	$439 million	(McCrank & Finkle, 2018)
Home Depot	$62 million	(Vinton, 2014)
Sony	$15 million	(Hackett, 2015)
Target	$148 million	(Vinton, 2014)
Yahoo*	$350 million	(Paul, 2017)

*cost represents reduction in sales price as purchased by Verizon

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

Though the numbers associated with the security breaches are large, they may appear less significant when framed relative to overall firm revenue. For example, the security breach costs were estimated at less than 2% of Sony's 2014 sales, less than 0.1% of Target's 2014 sales, and less than 0.01% of 2014 sales for Home Depot (Hackett, 2015). Even regarding Equifax's breach which is considered to be the most expensive in history, at $439 million, after the $125 million covered by insurance (McCrank & Finkle, 2018), the remaining $314 million is only 9.3% of 2017 revenue of $3.36 billion, and Equifax still declared net income of $587 million for 2017. Another path to view the damage caused by security breaches is to consider market reactions to the announcement of the data breach. For the publicly traded firms that announced the discovery of a large-scale data breach, Table 3 shows the stock's closing price on the last trading day before the firm announced the data breach, the first full day after the announcement and six months after the announcement.

Although limited in sample size, results in Table 3 appear to indicate that there are not crippling immediate, or long-term, impacts on the market value of a firm after experiencing a data breach. In fact, over the six months following the disclosure of a security breach, the average change over the six-month period was positive. The notion that data-related breaches are not particularly damaging to market value has some further support, as research finds that functional information technology failures, such as websites failing to work properly, are much more damaging to a firm's market value (Goldstein et al., 2011) than are failures related to data assets (Acquisti, Friedman, & Telang, 2006; Cavusoglu, Mishra, & Raghunathan, 2004). More specifically, findings suggest that public disclosure of security breaches results in an immediate negative impact on a firm's market value, but that this negative impact dissipates over time (Acquisti et al., 2006).

The financial data, though limited, seem to suggest that accepting the risk of breaches is a financially viable alternative for firms, at least from a profit maximizing shareholder perspective. In spite of the significant direct expenses incurred by breaches (see Table 2), these expenses might be relatively small in relation to overall firm revenue, and the investors in these firms, on average, seem willing to accept these expenses, as the average share price increased by a little over 4% over the six months following the breach (see Table 3). If direct financial ramifications are limited and market forces do not punish data breaches long-term, then the purely rational decision for managers might be to underinvest and deprioritize information security and simply accept the risk of data breaches unless sensitive or idiosyncratic data represents a key strategic resource which the firm could not be competitive if it is lost.

On one hand, though limited in sample size, the findings indicated in Table 3 would seem to indicate that for large, publicly traded firms, the strategic uncertainties from IT security risks can potentially be addressed by simply accepting the risks of suffering a security breach. From a purely economic perspective, as part of a risk management analysis, risk analysts estimate the probability of relevant security breach scenarios, the cost associated with each, and compare those estimated costs with the necessary security investments. If the cost of investing in security outweighs the estimated costs (the probability of a breach multiplied by the estimated cost) of an associated

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

Table 3: Market Impact of Disclosing Security Breach

Organization	Date Breach Disclosed by Organization	Closing Stock Price Trading Day Before Announcement	Closing Stock Price Trading Day After Announcement	Percent Change	Stock Price Six Months After Announcement	Percent Change
Anthem	2/13/2015	$142.00	$141.76	-0.17%	$149.69	+5.14%
Community Health Systems	8/18/2014	$42.15	$42.48	+0.78%	$40.42	-4.10%
eBay	5/21/2014	$51.96	$51.50	-0.89%	$54.42	+4.52%
Equifax	9/7/2017	$141.39	$123.23	-12.84%	$121.12	-14.34%
Home Depot	9/8/2014	$91.61	$88.93	-3.01%	$115.25	+20.51%
JPMorgan Chase	10/2/2014	$59.77	$60.30	+0.88%	$60.52	+1.24%
Sony	11/24/2014	$21.24	$21.63	+1.80%	$31.63	+32.85%
Target	12/19/2013	$63.55	$62.49	-1.70%	$58.74	-8.19%
Verizon	3/24/2016	$52.91	$53.40	+0.93%	$52.56	-0.66%
Average Change:				-1.58%		+4.11%

security failure, it would make economic sense for the firm to accept the risk of a breach. From a shareholder perspective, at least, a cursory evaluation would indicate accepting security risks as a viable scenario.

However, such a purely financial perspective on the cost of security breaches creates a moral hazard, because the firm choosing not to invest in increased security is simply transferring risk to another party who is not knowingly or willingly accepting that risk, such as their customers, employees or business partners. This quandary invites consideration of a profit maximizing shareholder perspective against that of a profit optimizing stakeholder perspective (Smith, 2003). Furthermore, if many firms choose to accept these risks it likely creates a vicious cycle, wherein breaches amongst these firms enable and drive more breaches amongst firms that are investing to minimize security risks.

From a strategic perspective, financially surviving a security breach would appear to be contingent on the level of resources available to the firm. As one security consultant writes:

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

> "Companies don't go out of business due to a cybersecurity breach," say several well-versed cybersecurity experts. When I give them counter-examples to disprove their point, they list it as an aberration.
>
> Here's a less catchy but more accurate statement: "Large companies usually don't go out of business due to a large cybersecurity breach. They can often get by with their CEO, CIO, and/or CISO getting fired. Medium and small companies can go out of business or go bankrupt due to a cybersecurity breach." (Black, 2019)

As a result, it appears that large firms with ample resources can potentially be cavalier about information security-related uncertainties. However, given that 60% of small business are reported to be bankrupt within 6 months of a breach (Miller, G., 2016) and that the average cost of a breach approaches $4 million (Ponemon, 2018), executives within small and medium-sized firms should be take these uncertainties seriously and sensibly invest in information security seriously to ensure the long-term viability of their business.

4. ***Traditionally, top management executives were not held individually responsible for breaches, but recent cases suggest otherwise.***

In the past, top management executives were relatively insulated from the fallout of information security failures. Strategic uncertainties related to information security and IT operations were, and still are, complicated and difficult to grasp. Since top managers were not directly involved in the day-to-day IT activities that left a vulnerability exploited in a breach or failed to identify an ongoing breach, there was a perception that they were not individually responsible. It is impractical to expect top managerial executives to be tightly involved in the design and arrangement of specific information security policies or tools, as it is almost certainly outside their area of expertise and not necessarily a cost effective use of their time (Ross & Weill, 2002; Weill & Ross, 2004). Because of the perceived distance between C-level executives and information security practices, repercussions for information security breaches rarely reached the top echelons of management.

Now, it appears corporate level executives are going to be held to a higher level of responsibility for information security failures (Misson, 2015). As cited above, for large firms top executives, like the CEO or CIO might serve as a potential scapegoat in the fallout of a security breach (Black, 2019). In several recent instances, a variety of top executives have left their positions after significant security breaches, including the Target CEO (O'Connor, 2014), the Sony Pictures co-chairman (Pallotta, 2015), two Equifax executives (Logan, 2017), the Yahoo head lawyer (Goel, 2017), and the Ashley Madison CEO (Zetter, 2015a). In another instance, when Uber data was breached, Uber paid the hackers $100,000 to delete the stolen data, which ultimately resulted in the ousting of the Uber Chief Security Officer and a top deputy (Newcomer, 2017). In fact, recent reports suggest that in almost one-third (31%) of data breaches, a C-level manager lost their job (Barker, 2018; Pankov, 2018). This recent shift towards holding higher level executives

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

accountable for security failures suggests a change in perspective regarding the role of top executives in preventing breaches. Instead of assuming information security is beyond the scope of top-level executive's responsibility, the perspective seems to be changing towards expecting top level executives to set the tone and overall strategy of the organization towards information security. Now, top executives are more likely to be considered culpable when the information security strategy fails (NeSmith, 2018).

Given the number of factors that seem to push large firms with ample resources towards simply accepting the risk of security breaches, the tendency towards holding top management personally accountable should steer firms towards other risk management decisions. These decisions might be to minimize risk by investing in information security or to transfer risks to service or insurance providers. As a result, we would expect that decision-makers may make more conservative decisions regarding information security investment decisions than a purely economic perspective would suggest. In other words, top managers should pay more attention to security issues, as desired by their IT personnel (Ismail, 2017), and invest more time planning for security incidents (Forrest, 2018)

Environmental Context and Externalities

5. ***Security breaches are becoming a more universally common experience and may become more accepted as an inevitability in the information age.***

Given the massive numbers associated with many of the high-profile data leaks, where the number of people impacted regularly ranks in the millions and hundreds of millions, security breaches are becoming a more universally common experience (see Table 1). Breaches include the exposure of data from 3 billion Yahoo user accounts (Larson, 2017), 147 million Americans via Equifax records (Fung, 2018; O'Brien, 2017), and millions of social media user accounts like Tumblr (Kovacs, 2016) and LinkedIn (Hackett, 2016). Millions of consumers and employees are impacted by security breaches on a regular basis, and security attacks are common for businesses; research suggests that 43% of companies experienced a data breach in 2014 (Weise, 2014a). In fact, a recent report suggests that data breaches are occurring at a faster rate than ever before, with breaches in the first half of 2017 almost 30% higher than the same period in 2016 (Weisbaum, 2017).

Perversely, the increasing commonality of security breaches (Brino, 2012; Hulme, 2014; Roettgers, 2015) may have counterintuitive consequences. Some indications suggest people are becoming desensitized to the threat of security breaches and information leaks because such breaches are beginning to feel commonplace (Crosman, 2014). According to Jake Kouns, chairman of the Open Security Foundation, "There are so many breaches going, at some point we think data breaches are going to jump the shark and no one's going to care anymore. We'll have that fatigue of, 'Another breach – what do I care?'" (cited in Crosman, 2014).

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

In fact, given that breaches are becoming so seemingly commonplace and so large, users may perceive a certain level of psychological safety being only one person among 10 or 100 million records leaked. As the number of leaked files increases over time, those impacted by the leaks may feel a comparatively lower level of risk given the significant number of people effected. In other words, if an individual has personal data leaked in a breach impacting only 100 people, the risk of their information being used for identity theft, fraud or another crime would appear much more likely than for a breach impacting 100 million people. The large scale of the breaches make it seem statistically less likely that any individual's credentials will be used in a criminal manner.

Finally, there may be shifting social standards in terms of the ethical acceptability of publicly displaying and discussing hacked or leaked documents. While public consumption of leaked documents is not a universally accepted practice, in recent years, leaked documents from a variety of government and corporate entities have begun appearing online at various locations, such as WikiLeaks (www.wikileaks.org), which serve as public clearinghouses for distributing such material. For example, WikiLeaks posted the 170,000+ emails and 30,000+ corporate documents leaked via the Sony Pictures hack, and, as a result, individuals and media entities have analyzed and discussed private emails sent by many high profile individuals, including executives such as then-CEO Amy Pascal and Hollywood celebrities (Roettgers, 2015). In a similar instance, the user data and corporate emails leaked as a result of the Ashley Madison hack have been analyzed and discussed on public media websites to present arguments concerning misleading business practices (Newitz, 2015). In a more controversial example, former intelligence contractor Edward Snowden, who leaked U.S. intelligence materials to expose surveillance programs, is considered by some to be a traitor but by others to be a hero (Rasmussen, 2013).

Though this topic is difficult to distill into specific guidance for management, it does raise interesting questions and quandaries for managers. Long-term, organizations and decision-makers ought to consider their role in the gradual transition towards a society where security breaches and exposure of sensitive data and personal information becomes more commonplace. Although businesses will always have incentive to protect their own sensitive data and intellectual property, if societal norms change to where exposure of *customer data* becomes "business as usual," then incentives to protect and secure customer data are reduced. So long as financial penalties and associated damages are high, businesses have significant financial incentive to carefully protect customer data. If cultural norms change toward accepting the continual exposure of customer data en masse, the financial motivation to protect customer data might eventually weaken. This would economically incentivize the risk management decision to accept risk instead of minimizing or transferring risk.

In the face of changing societal standards, this conversation invites consideration of the shareholders versus stakeholders debate (Smith, 2003). The shareholders perspective suggests that management has an obligation to maximize the return on investment for business owners—the shareholders. The stakeholder perspective suggests that management has a moral obligation to balance the best interests of the shareholders with the best interests of all major stakeholders in the

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

business, including employees, customers, business partners, community members, and so forth. In the face of increasing rates of security breaches (Weisbaum, 2017), firms will need to decide if they intend to surrender to the seeming inevitability of security breaches or to invest resources and energy into protecting sensitive data. Furthermore, firms should consider that their approach to information security does not occur in isolation. The extent to which a firm invests in security impacts the external business environment by either increasing the rate of breaches through lax standards or minimizing the rate of breaches through investing in security.

6. ***Even though increasing security may be in the best interest of the consumers and employees, consumers and employees may not want increased security.***

Customer data is one of the most notable pieces of data stolen in numerous high-profile breaches. However, despite the clear risks posed by information security breaches, customers and employees may both resist or dislike initiatives to increase information security that directly impact their processes or user experience. Such attempts to increase security may often be met with user resistance or avoidance behaviors. Organizations can try to increase information security by requiring longer, more complicated passwords, by requiring that passwords are changed more often, or by creating multiple security checks to verify an individual's identity. These attempts to increase security may actively frustrate users and potentially discourage them from using the service in the first place, which could hamper an organization's growth and profitability.

Furthermore, organizations seeking to enhance information security could consider using more advanced security tools, such as two-factor authentication, where a user must possess a second authenticating device (such as an authorized cell phone) in order to log in to a system, or could implement biometric tools, such as a fingerprint scanner, to verify credentials. However, not all consumers are educated about the use of more elaborate security countermeasures or would necessarily be motivated to absorb the cost of extra time and money to implement the added security.

Organizations have a lot more power over securing the behavior of their employees, and employers can require compliance with a variety of information security protocols, such as the changing of passwords or the use of encryption services to access corporate networks. However, increased security may be in the best interest of the organization and even of the employees, who may risk the exposure of personal data (e.g., Pagliery, 2014). Employees may even knowingly deactivate or circumvent security protocols due to their potential negative impact on their individual performance and productivity (Ruighaver, Maynard, & Chang, 2007; Workman, Bommer, & Straub, 2008). In other words, there are instances where increased security protocols, which are in the best interest of the organization and all employees, run cross-purpose to the immediate self-interest of the employee desiring to maximize their own short-term productivity.

Further complicating the issue of security behaviors are the various motivations and desires of the users. There is also the risk of deliberate acts of information theft (Whitman, 2003) and that individuals with access to organizational systems participate in a security breach to damage or

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

steal from their employer (Krebs, 2015). Finally, in rare instances, employees might intentionally leak data to serve as a whistleblower on what they perceive to be illegal or unethical organizational practices, such as the case of Edward Snowden leaking information on U.S. intelligence and surveillance programs (Mazzetti & Schmidt, 2013). Therefore, decision-makers must account for the various shortcomings and diverse motivations of organizational users and personnel with access to secure systems.

Implementing security policies concerning employees and customers are separate, but related issues. In both instances, bolstering security processes with more stringent requirements may inhibit use of the systems the processes are intended to protect. For example, an organization might require employees to change passwords every 30 days and to use two-factor authentication to validate access to sensitive systems. In return, employees might leave passwords written on a note near their computer or might avoid using the system altogether. In order to garner employee support for stringent security policies, organizations may need to engage in education and training campaigns to convince users of the necessity of tight security. Employees may need to be convinced that security is the responsibility of every employee. Education campaigns may benefit from convincing employees that security is in their own best interest, as these practices protect their own credentials (which could potentially be used to access other accounts held by the individual, such as banking or financial information) as well as their long-term job security by protecting the firm's ongoing processes.

Regarding implementation of security processes that protect customers but require customer involvement (i.e. log-in credentials), firm operations are somewhat limited since the firm cannot dictate security behaviors to a customer in the same way that requirements can be placed on employees. For instance, businesses with websites or smartphone apps that have long, complicated password requirements or require two-factor authentication may discourage many potential customers from patronizing their site or app in the first place. The business needs to balance security with ease of access and the risk of losing customers. One approach is to provide customers with the option to leverage advanced security options, like two-factor authentication, and then strongly encourage customers to make use of it. In this way, the firm transfers some risk to the customer by providing them with the option to use strong security practices but gives them the ability to decline if they do not wish to do so.

Throughout this paper, we have treated information security breaches as a strategic uncertainty that creates significant risk for firms. However, in light of the proliferation and seeming inevitability of security breaches, there might be a significant opportunity for firms to position themselves based on security. As more consumers and businesses become aware of the significant threat posed by insecure infrastructures and platforms, concerned users may be driven to seek products and services that prominently feature security as a core component of the product or service. For example, email provider ProtonMail (protonmail.com) offers secure and private email communications. The success of positioning an organizational strategy partly or entirely on security features would likely be contingent upon the extent to which customers become numb to

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

the repeated announcement of large-scale breaches. If customers are largely apathetic, such a strategy would likely only succeed as a niche positioning strategy—targeting the few who desire security and are willing to pursue it. If customers become more aware of security risks and the majority desire security, then such a strategy would have potential as a mass market strategy.

LIMITATIONS AND FUTURE RESEARCH

We do acknowledge the limitations of this paper. Ideally, primary data collected directly from breached firms would offer deeper insight into the decision-making processes before, during and after security breaches. However, gaining access to such data may be extremely difficult. Additionally, we sought to offer practical advice for managers when engaging in decision-making regarding investments in information security. Our intention is to drive more informed conversation between top-level decision makers and IT personnel. Unfortunately, a complete and in-depth discussion of the risk management process is outside the scope of this paper, but we hope the topics discussed here will inform more intelligent decision-making when engaging in risk management analysis and planning.

Future research should consider expanding upon the conceptual framework (see Figure 1) that we advanced. To the best of our knowledge, this is the first attempt to develop a framework focused on the strategic consequences of information technology and security failures, whereas taxonomies of specific IT operational failures are readily available. We hope the strategic focus of the framework will provide a foundation for further scholarship in this area. Additionally, future research should consider further investigation of the specific problem issues we addressed. For example, the trends towards more security breaches and indicators of "breach fatigue" among consumers suggest changing cultural attitudes towards the consequences of such breaches. Future research should consider evaluating the potential for changes in consumer and investor attitudes towards breaches and if they correlate with reduced consequences for firms following breaches.

CONCLUSION

Security breaches are a complex and continually changing phenomenon that create a unique strategic problem for organizational decision-makers. There are numerous factors that exacerbate the level of strategic uncertainty associated with the pursuit of information security, and security breaches seem to be an inevitability for many organizations. Although the financial repercussions may be limited in the long-term, recent history suggests that organizations are beginning to hold top executives responsible. As a result, it becomes imperative for top decision-makers to understand why security breaches are an ongoing threat and to have a grasp on the many factors that make such information security threats hard to understand and manage.

The Coastal Business Journal

ISSN: 2163-9280 Fall 2019
Volume 17, Number 1

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Allaire, Y., & Firsirotu, M. E. (1989). Coping with strategic uncertainty. *MIT Sloan Management Review, 30*(3), 7.

Anderson, R. (2001). *Why information security is hard - An economic perspective.* Paper presented at the Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual.

Barker, I. (2018). 32 percent of data breaches lead to executive job loss. Retrieved October 10th, 2018, from https://betanews.com/2018/09/14/data-breach-executive-job-loss/

Black, R. (2019). Cybersecurity Breach Bankruptcy: It Does Happen. Retrieved February 7, 2019, from https://fractionalciso.com/cybersecurity-breach-bankruptcy/

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms.

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE software, 8*(1), 32-41.

Bose, I., & Leung, A. C. M. (2008). Assessing anti-phishing preparedness: A study of online banks in Hong Kong. *Decision Support Systems, 45*(4), 897-912. doi: 10.1016/j.dss.2008.03.001

Brino, A. (2012). Security experts warn of increasing data breaches and privacy risks. Retrieved November 25, 2014, from http://www.govhealthit.com/news/underwriting-experts-warn-increasing-data-breaches-and-privacy-risks

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Cebula, J. L., & Young, L. R. (2010). A taxonomy of operational cyber security risks: CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Collins, K. (2015). A Quick Guide to the Worst Corporate Hack Attacks. Retrieved 2015, July 17, from http://www.bloomberg.com/graphics/2014-data-breaches/

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

Courtney, H., Kirkland, J., & Viguerie, P. (1997). Strategy under uncertainty. *Harvard Business Review, 75*(6), 67-79.

Cromwell, S. E., & Kolb, J. A. (2004). An examination of work-environment support factors affecting transfer of supervisory skills training to the workplace. *Human resource development quarterly, 15*(4), 449-471.

Crosman, P. (2014). Eight Lessons for Banks from the Data Breaches of 2014. Retrieved December 5, 2014, from http://www.americanbanker.com/news/bank-technology/eight-lessons-for-banks-from-the-data-breaches-of-2014-1071465-1.html

Elenkov, D. S. (1997). Strategic uncertainty and environmental scanning: The case for institutional influences on scanning behavior. *Strategic Management Journal, 18*(4), 287-302.

Facteau, J. D., Dobbins, G. H., Russell, J. E., Ladd, R. T., & Kudisch, J. D. (1995). The influence of general perceptions of the training environment on pretraining motivation and perceived training transfer. *Journal of Management, 21*(1), 1-25.

Fiegerman, S. (2016a). Yahoo says 500 million accounts stolen. Retrieved January 10, 2018, from https://money.cnn.com/2016/09/22/technology/yahoo-data-breach/index.html

Fiegerman, S. (2016b). Yahoo says data stolen from 1 billion accounts. Retrieved January 10, 2018, from https://money.cnn.com/2016/12/14/technology/yahoo-breach-billion-users/index.html

Forrest, C. (2018). Report: 77% of companies don't have a consistent cybersecurity response plan. Retrieved February 7, 2019, from https://www.techrepublic.com/article/report-77-of-companies-dont-have-a-consistent-cybersecurity-response-plan/

Fung, B. (2018). 145 million Social Security numbers, 99 million addresses and more: Every type of personal data Equifax lost to hackers, by the numbers. Retrieved October 4, 2018, from https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/?noredirect=on&utm_term=.39f308c783a8

Goel, V. (2017). Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack. Retrieved August 12, 2017, from https://www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-bonus.html

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems, 12*(9), 1.

Grow, B., Epstein, K., & Tschang, C. (2008). The New E-Spionage Threat. Retrieved April 20, 2012, from http://www.bloomberg.com/bw/stories/2008-04-09/the-new-e-spionage-threat

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

Hackett, R. (2015). How much do data breaches cost big companies? Shockingly little. Retrieved August 12, 2015, from http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/

Hackett, R. (2016). LinkedIn Lost 167 Million Account Credentials in Data Breach. Retrieved April 6, 2017, from http://fortune.com/2016/05/18/linkedin-data-breach-email-password/

Hulme, G. V. (2014). Survey shows the cost of security breaches is on the rise. Retrieved December 2, 2014, from http://www.csoonline.com/article/2689346/big-data-security/survey-shows-the-cost-of-security-breaches-are-on-the-rise.html

Ismail, N. (2017). Is cyber security still not a top boardroom priority? Retrieved January 31, 2019, from https://www.information-age.com/cyber-security-still-not-top-boardroom-priority-123468999/

Issac, M., Benner, K., & Frenkel, S. (2017). Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data. Retrieved February 9, 2018, from https://www.nytimes.com/2017/11/21/technology/uber-hack.html

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626.

Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS Quarterly, 32*(1), 127-157.

Korosec, K. (2018). What Amazon lost (and made) on Amazon Prime Day. Retrieved 10/3/2018, 2018, from https://techcrunch.com/2018/07/18/amazon-prime-day-outage-cost/

Kovacs, E. (2016). 65 Million Users Affected by Tumblr Breach. Retrieved October 4, 2017, from https://www.securityweek.com/65-million-users-affected-tumblr-breach

Krebs, B. (2014). Target Hackers Broke in Via HVAC Company. Retrieved April 19, 2015, from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Krebs, B. (2015). Online Cheating Site AshleyMadison Hacked. Retrieved November 2, 2015, from http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). *School of phish: a real-world evaluation of anti-phishing training.* Paper presented at the Proceedings of the 5th Symposium on Usable Privacy and Security.

Larson, S. (2017). Every single Yahoo account was hacked - 3 billion in all. Retrieved January 27, 2018, from https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html?iid=EL

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

Logan, B. (2017). 2 top Equifax execs are out after a massive hack that exposed 143 million Americans' financial data. Retrieved November 16, 2017, from https://www.businessinsider.com/equifax-cyberattack-hackers-executives-retiring-2017-9

Mazzetti, M., & Schmidt, M. S. (2013). Ex-Worker at C.I.A. Says He Leaked Data on Surveillance. Retrieved February 7, 2015, from http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html

McCarthy, K. (2015). 32 Data Breaches Larger Than Sony's in the Past Year. Retrieved August 3, 2015, from http://www.huffingtonpost.com/kyle-mccarthy/32-data-breaches-larger-t_b_6427010.html

McCrank, J., & Finkle, J. (2018). Equifax breach could be most costly in corporate history. Retrieved June 12, 2018, from https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257

McGee, M. K. (2014). Hospital Chain Breach: How Expensive? Retrieved October 2, 2015, from http://www.databreachtoday.com/hospital-chain-breach-how-expensive-a-7252

Miller, G. (2016). 60% of small companies that suffer a cyber attack are out of business within six months. Retrieved February 7, 2019, from https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

Miller, K. D. (1992). A framework for integrated risk management in international business. *Journal of international business studies*, *23*(2), 311-331.

Misson, T. (2015). C-Level Executives No Longer Immune to the Effects of a Security Breach. Retrieved August 19, 2015, from https://www.securestate.com/blog/2015/07/31/c-level-executives-no-longer-immune-to-the-effects-of-a-security-breach

Mitnick, K. D., & Wimon, W. L. (2005). *The Art of Intrusion*: Wiley.

Narcisi, G., & Kuranda, S. (2016). Telecom Partners Say Cloud Security Is Top Of Mind In Wake Of Verizon Breach. Retrieved August 23, 2016, from https://www.crn.com/news/security/300080151/telecom-partners-say-cloud-security-is-top-of-mind-in-wake-of-verizon-breach.htm

NeSmith, B. (2018). CEOs: The Data Breach Is Your Fault. Retrieved October 1st, 2018, from https://www.forbes.com/sites/forbestechcouncil/2018/06/26/ceos-the-data-breach-is-your-fault/#4e05471258b0

Newcomer, E. (2017). Uber Paid Hackers to Delete Stolen Data on 57 Million People. Retrieved July 2, 2018, from https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Newitz, A. (2015). Ashley Madison Code Shows More Women, and More Bots. Retrieved October 8, 2015, from http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

O'Brien, S. A. (2017). Giant Equifax data breach: 143 million people could be affected. Retrieved November 12, 2017, from https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

O'Connor, C. (2014). Target CEO Gregg Steinhafel Resigns In Data Breach Fallout. Retrieved May 2, 2015, from http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/

Ocasio, W. (1997). Towards an Attention-Based View of the Firm. *Strategic Management Journal, 18*(Special Issue), 187-206.

Ocasio, W., & Joseph, J. (2005). An Attention-Based Theory of Strategy Formulation: Linking Micro and Macro Perspectives in Strategy Processes. *Advances in Strategic Management, 22*(1), 39-62.

Osborne, C. (2015). Cost of Anthem's data breach likely to exceed $100 million. Retrieved July 19, 2015, from http://www.cnet.com/news/cost-of-anthems-data-breach-likely-to-exceed-100-million/

Pagliery, J. (2014). The Sony mega-hack: What you need to know. Retrieved December 9, 2014, from http://money.cnn.com/2014/12/09/technology/security/sony-hacking-roundup/

Pallotta, F. (2015). Amy Pascal out as Sony Pictures co-chair. Retrieved March 9, 2015, from http://money.cnn.com/2015/02/05/media/amy-pascal-resigns-sony/

Pankov, N. (2018). Businesses and personal data: In-depth analysis of practices and risks. Retrieved October 10th, 2018, from https://www.kaspersky.com/blog/data-protection-report/23824/

Paul, F. (2017). We finally know how much a data breach can cost. Retrieved March 9, 2018, from https://www.networkworld.com/article/3172402/security/we-finally-know-how-much-a-data-breach-can-cost.html

Ponemon, L. (2015). Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis'. Retrieved September 22, 2015, from https://securityintelligence.com/cost-of-a-data-breach-2015/

Ponemon, L. (2018). Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT. Retrieved July 30, 2018, from https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

Rasmussen. (2013). 12% See NSA Leaker Snowden As Hero, 21% As Traitor. Retrieved June 12, 2015, from http://www.rasmussenreports.com/public_content/politics/general_politics/june_2013/12_see_nsa_leaker_snowden_as_hero_21_as_traitor

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

Reisinger, D. (2014). eBay hacked, requests all users change passwords. Retrieved September 22, 2015, from http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/

Reuters. (2014). JPMorgan hack exposed data of 83 million, among biggest breaches in history. Retrieved August 9, 2015, from http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003

Roettgers, J. (2015). Sony Hack, One Year Later: Is Hollywood Prepared for the Next Attack? Retrieved November 7, 2015, from http://variety.com/2015/biz/features/sony-hack-anniversary-next-attack-1201631689/

Ross, J. W., & Weill, P. (2002). Six IT decisions your IT people shouldn't make. *Harvard Business Review, 80*(11), 84-95.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Smith, H. J. (2003). The shareholders vs. stakeholders debate. *MIT Sloan Management Review, 44*(4), 85-91.

Thomsen, S. (2015). Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online. Retrieved October 8, 2015, from http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

Vinton, K. (2014). With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's. Retrieved December 7, 2014, from http://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets/

Vinton, K. (2015). Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data. Retrieved July 18, 2015, from http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*: Harvard Business Press.

Weisbaum, H. (2017). Data Breaches Happening at Record Pace, Report Finds. Retrieved October 8th, 2018, from https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881

ISSN: 2163-9280 **Fall 2019**
Volume 17, Number 1

Weise, E. (2014a). 43% of companies had a data breach in the past year. Retrieved November 12, 2014, from http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/

Weise, E. (2014b). Health network reports 4.5 million patients had information hacked. Retrieved June 23, 2015, from http://www.usatoday.com/story/tech/2014/08/18/community-health-systems-hack-attack-45-million/14226421/

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46*(8), 91-95.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research, 25*(2), 385-400.

Zetter, K. (2015a). Ashley Madison CEO Resigns in Wake of Hack, News of Affairs. Retrieved September 22, 2015, from http://www.wired.com/2015/08/ashley-madison-ceo-resigns-wake-hack-news-affairs/

Zetter, K. (2015b). Hackers Finally Post Stolen Ashley Madison Data. Retrieved October 8, 2015, from http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/